



## Data Segmentation for Privacy

# VA/SAMHSA Pilot Brief

Sponsor(s)/Contact(s): Organization Name and Contact Name

SAMHSA [Richard.thoreson@samhsa.hhs.gov](mailto:Richard.thoreson@samhsa.hhs.gov)

Veterans Administration [Mike.Davis@va.gov](mailto:Mike.Davis@va.gov)

May 11, 2012



# PILOT BRIEF

- Develop and test (within a sandbox) standards-based management, exchange, adjudication, and enforcement of privacy consents, as services in support of the exchange of privacy protected C32/CCDA records.
- Testing involves interaction between ACS clones that are each loosely coupled to an instance of an open source, MU 1 certified, EHRs clone (Reference Electronic Record (REM), see below). This sandbox may test all “push” or “pull” scenarios defined in the IG.
- Mash up several Data Segmentation use cases to demonstrate key capabilities
  - [User Story 1.1B - Title 38 \(Pull/ Share All\)](#)
  - [User Story 1 C – Title 38 \(Pull/ Change Mind\) \*without HIO\*](#)
  - [User Story 1.1 A- Title 38 \(Push/ Share Partial\)](#)
  - [User Story 3 – \(Break the Glass\)](#)



# Committed Pilot Resources

- ✓ Establish Pilot Test Resources
  - SAMHSA Personnel & Contract Resources
    - OBHITA Open Source Contract (in 3<sup>rd</sup> year of planned 5 years) with FEISystems in Columbia, MD.
    - OBHITA consultant Ioana Singureanu, HL7 standards expert and systems architect
  - VA Resources
    - VA Contract (Edmonds SCI) *The actual scope of DS4P initiative testing will be limited by the short (4 month) testing period, and by a likely miss-match between this testing period and the VA Task Order*
    - Duane Decouteau, OASIS standards, systems architect, and programmer
    - Kathleen Connor , HL7 standards & IHE profiles expert
  - S&I Contractor technical assistance/support request
    - Facilitate collaboration with other DS4P pilots and with other participating DS4P experts

- **Create Working Reference Implementation for Policy Enforcement**

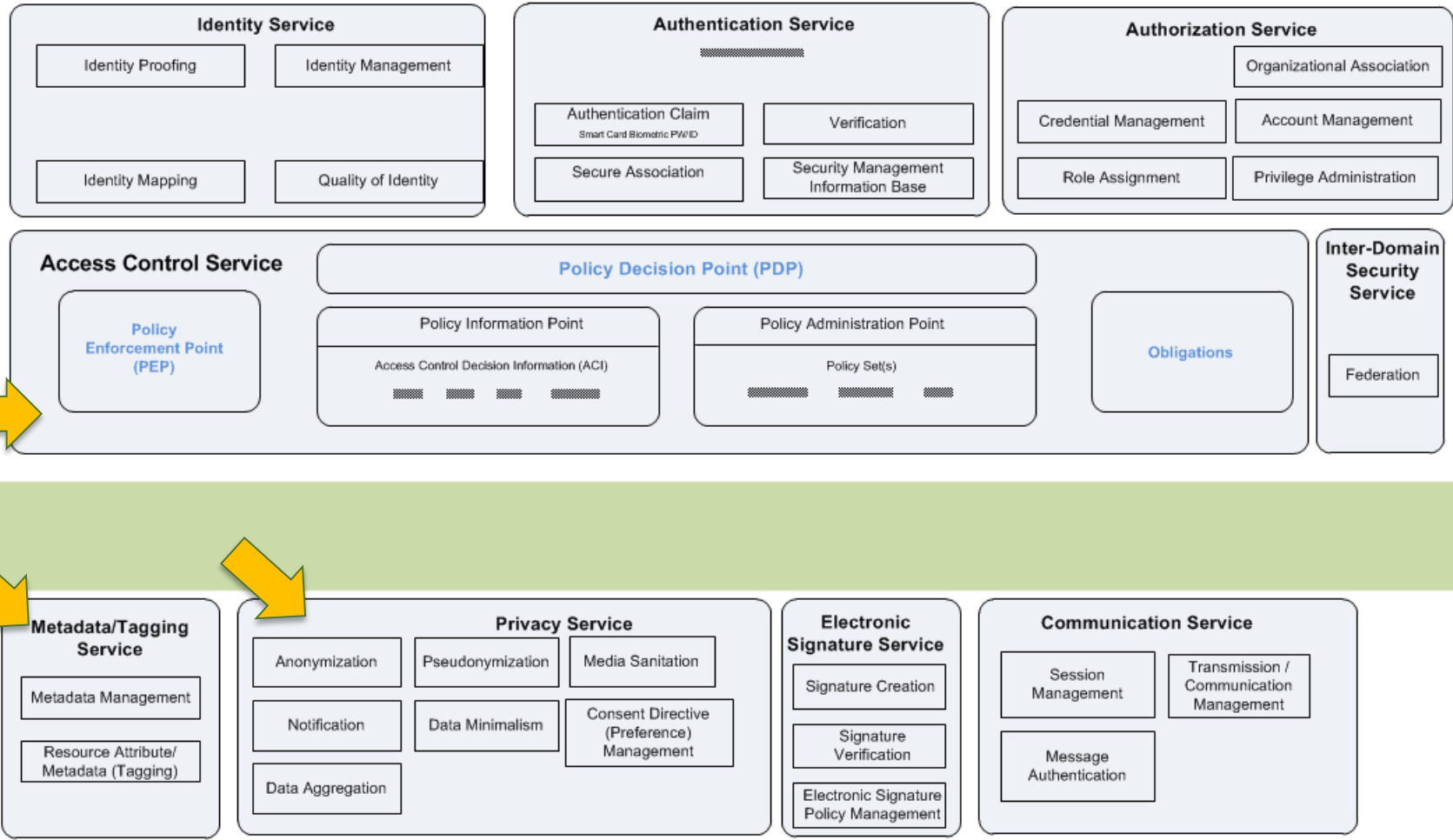
Privacy Law or Organizational Policy	Definition
Title 38 Section 7332	Title 38 Section 7332 Protected Information: Drug Abuse, Alcoholism, HIV, Sickle Cell
42 CFR Part 2	42 CFR Part 2 Behavioral Health Protected Information
HIV	Policy for handling HIV or AIDS information, which will be afforded heightened confidentiality.
PSY	Policy for handling psychiatry information, which will be afforded heightened confidentiality.
DIA	Policy for handling information related to a diagnosis, health condition or health problem, which will be afforded heightened confidentiality.
SICKLE	Policy for handling information related to sickle cell disease , which will be afforded heightened confidentiality.

# Architectural Placement of Security Services

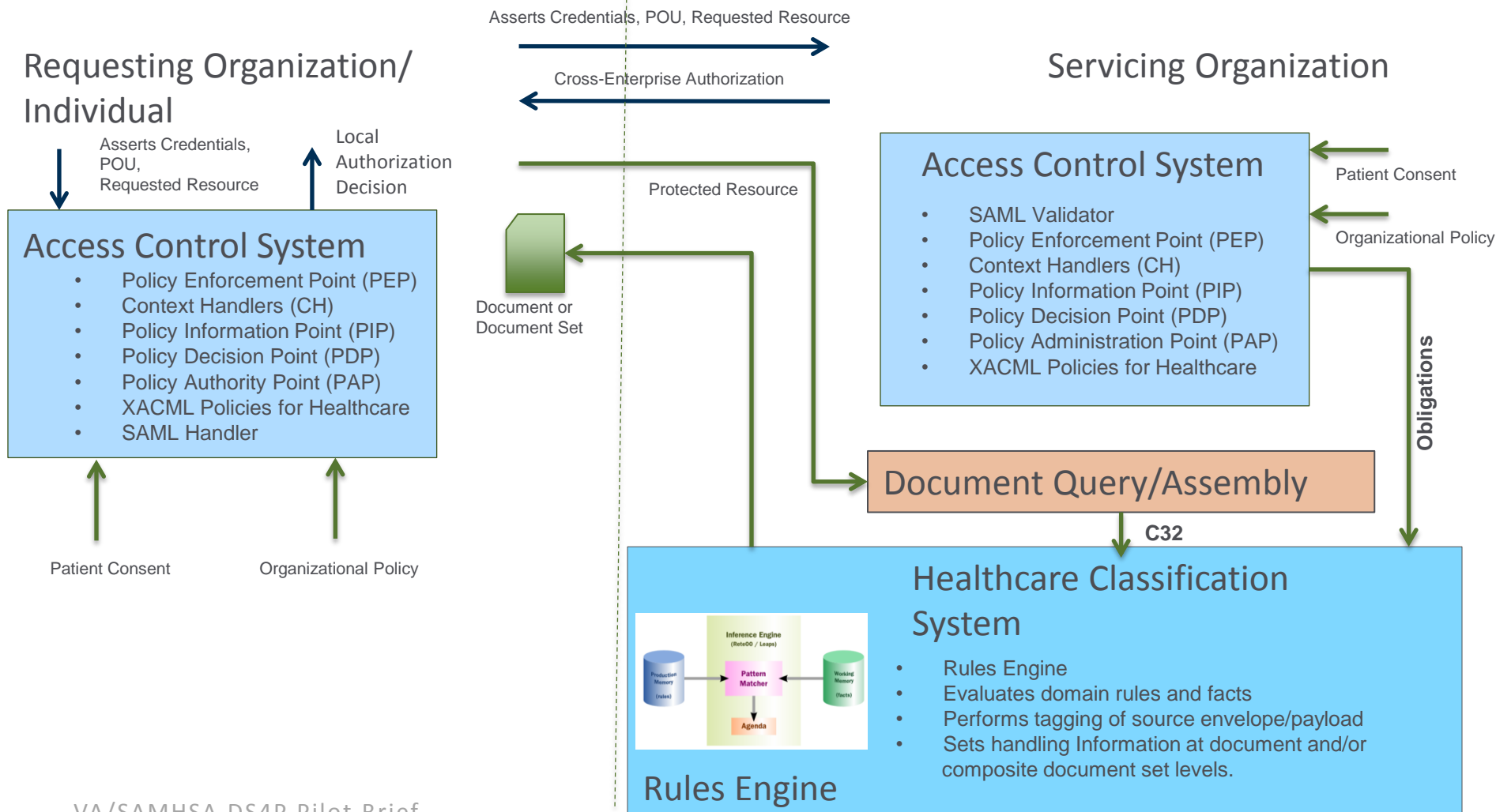
Identity and Access Management

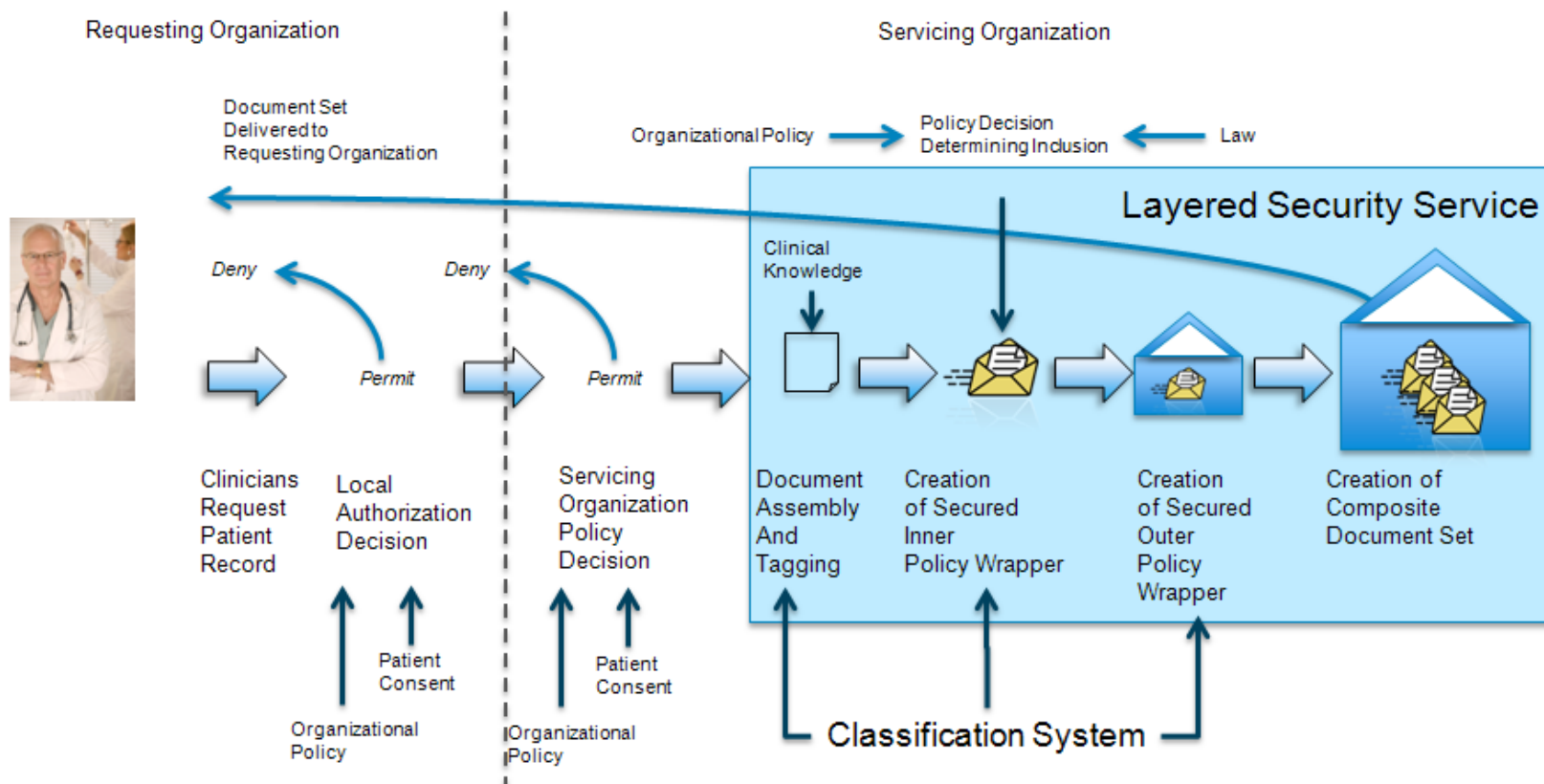


Business Logic



## Pull Use Cases – Request/Response



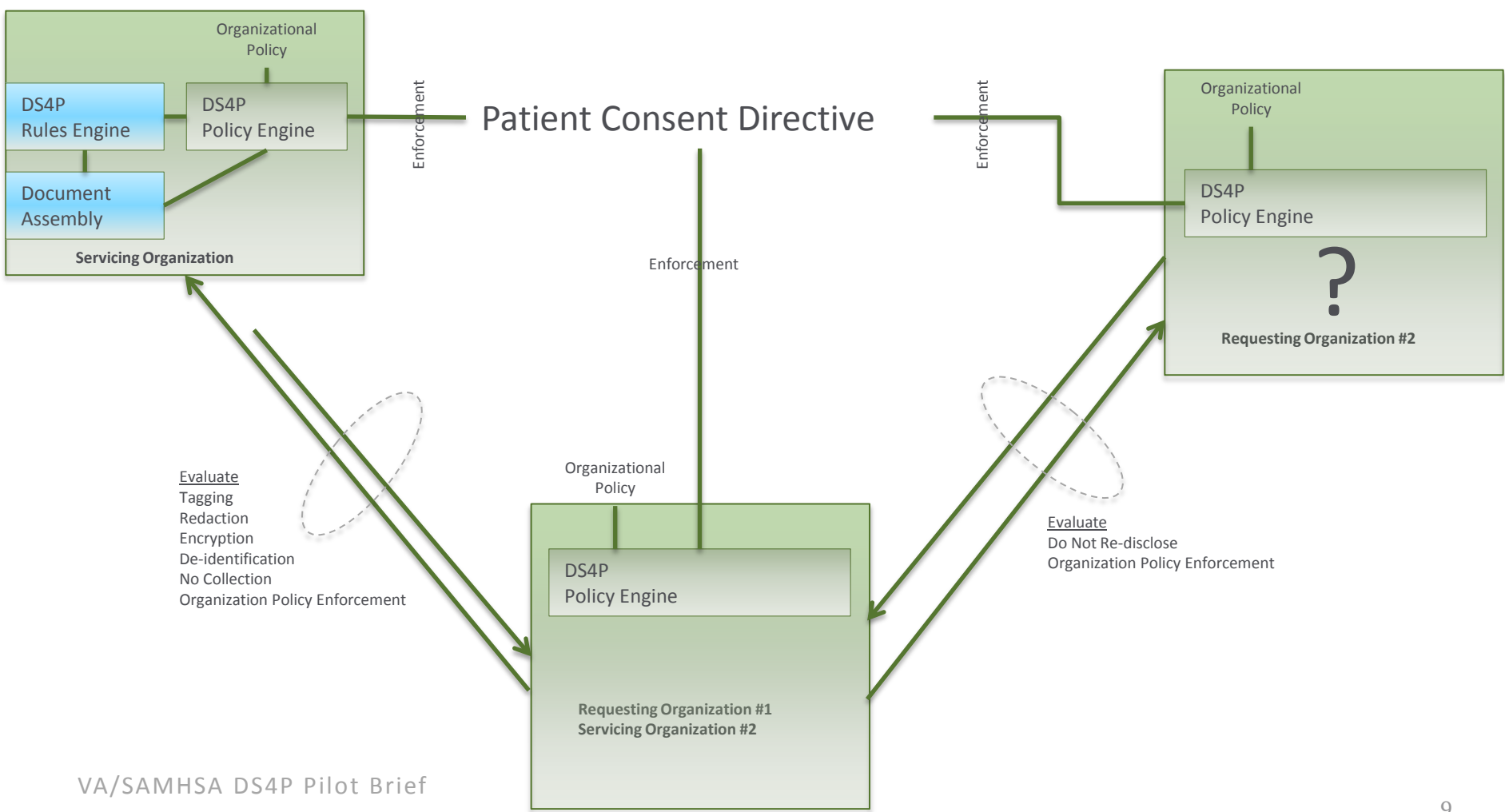






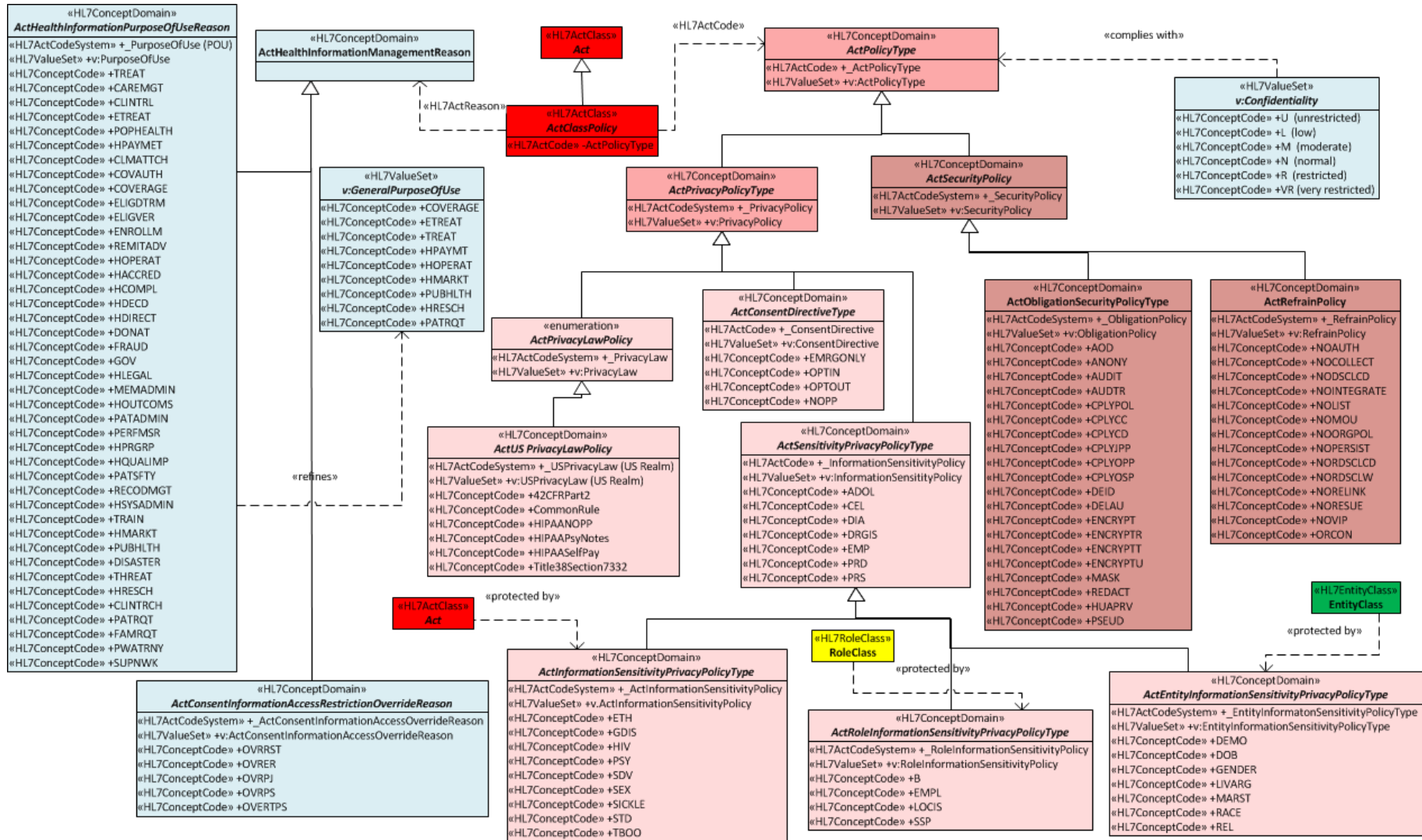


✓ Establish Pilot Test Environment





# Data Tags Based on HL7 Standard Vocabulary



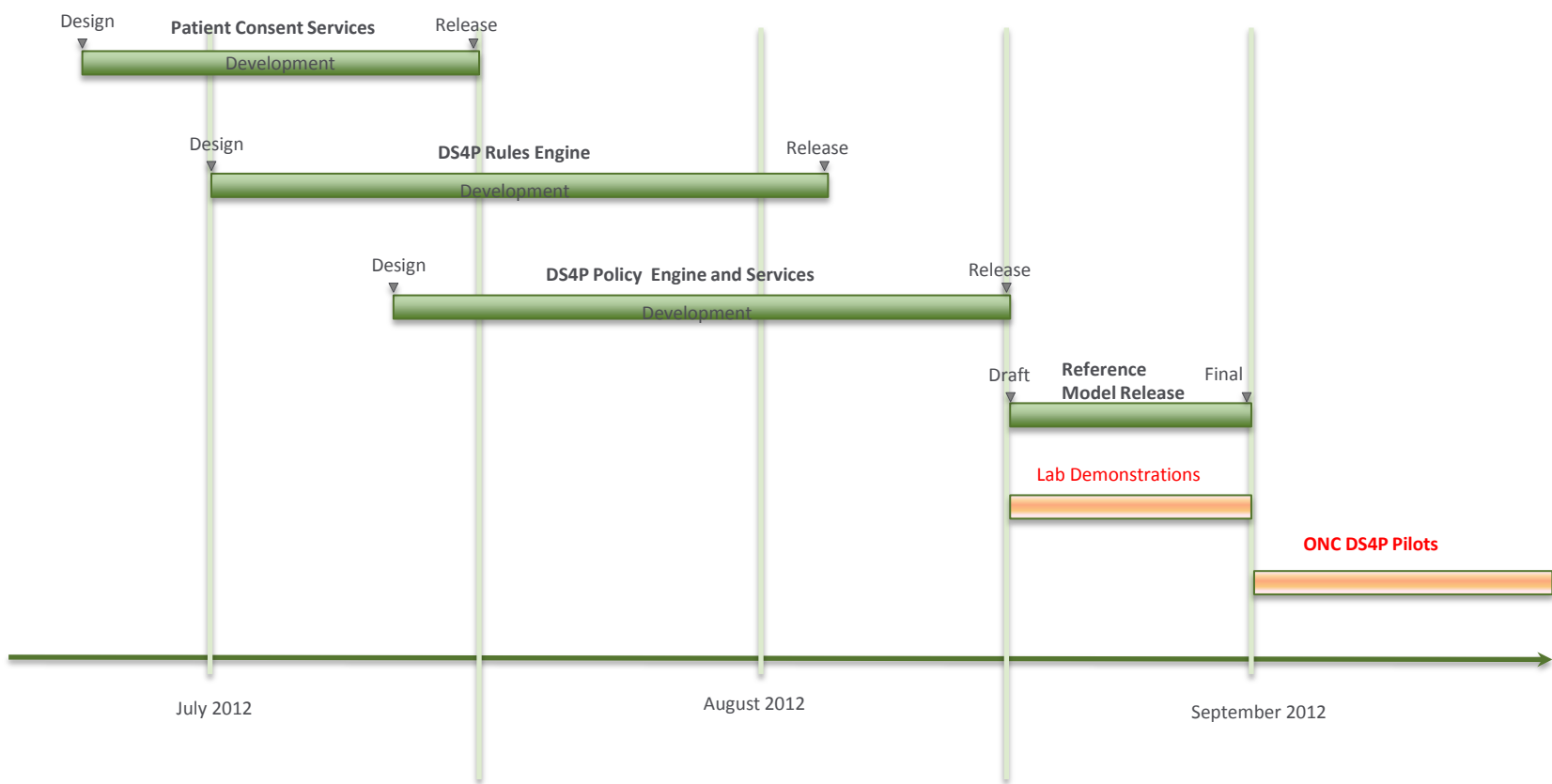


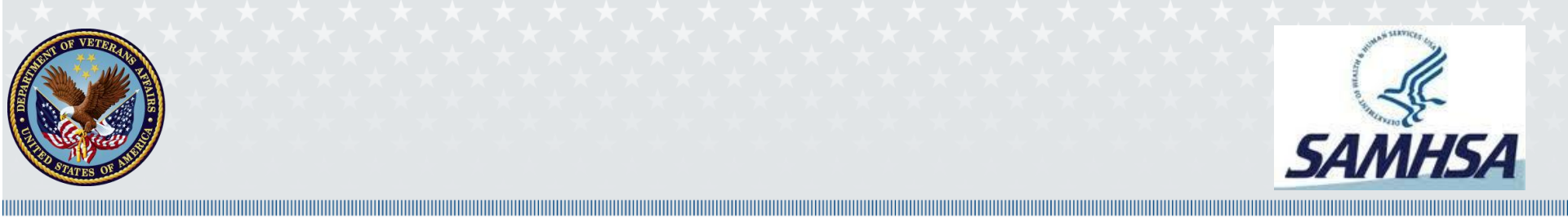
# Implementation and Testing

## ✓ Establish Pilot Implementation & Testing Process

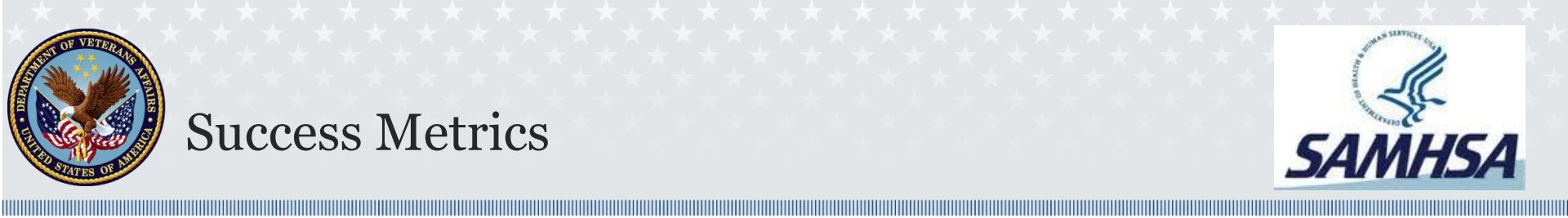
- SAMHSA/OBHITA-developed, MU1 Certified, Reference e-record Model (REM)
- VA developed HIMSS demonstration of automated privacy protection/VA NwHIN Reference Model/OASIS Reference Model

Proposed Timeline



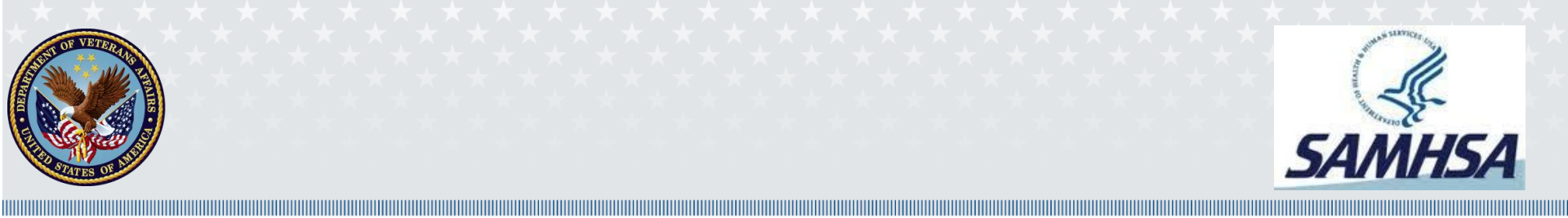


- Develop & Review Pilot Configuration (TBD)
- Documented & Reviewed Pilot Configuration Guide (TBD)
- Weekly Feedback on Use-Cases & IG Alignment (TBD)



# Success Metrics

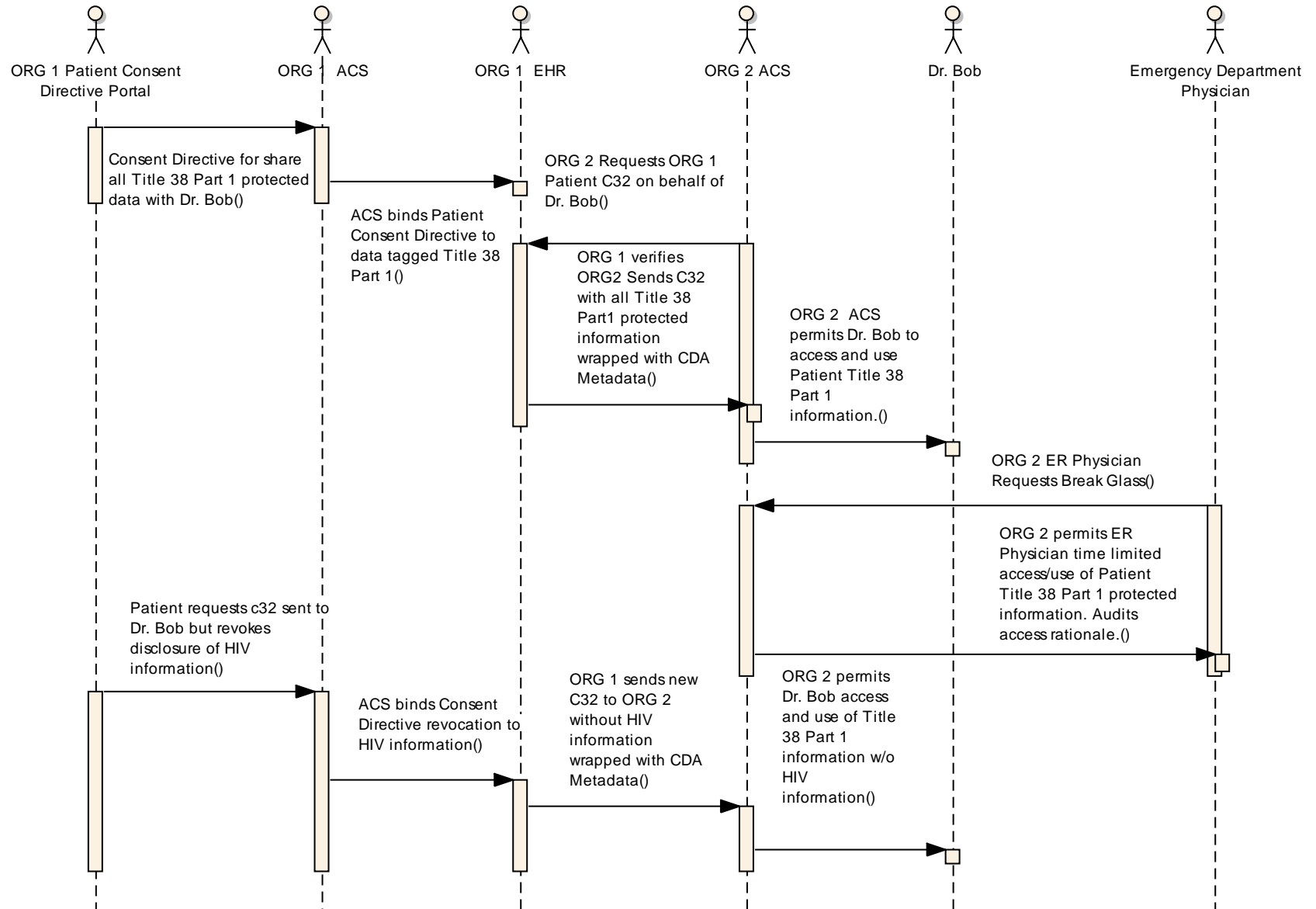
- Our long term goal is ubiquitous privacy consent management. Eventually, we plan to fully develop and test a production-ready ACS, as a cost effective way to manage privacy-protected exchange of clinical records for coordination care, for public health reporting, for billing (e.g. es-MD), and for PCAST-like sharing of sensitive records for services.
  - Automated Data Tagging (POU, Data Confidentiality, Data Sensitivity) per Classification Scheme
  - Align with Data Segmentation Use Case(s)
  - Demonstrate HIT Policy Committee Metadata Standards
    - Use HL7 security and privacy metadata in a CDA header for C32 envelope
  - Demonstrate compliance with Title 38 Part 1/42 CFR Part 2 required *prohibition against redisclosure* notification
  - Demonstrate segmentation of Title 38 Part 1/42 CFR Part 2 protected information in C32 based on tagging sensitive attributes



# BACKUP and For Further Information Slides



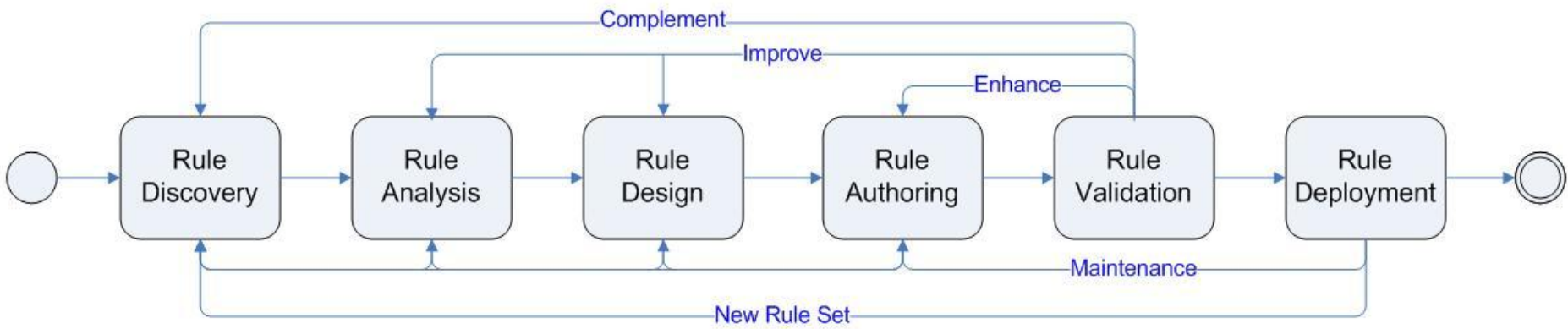
# sd Data Segmentation Sequence Diagram



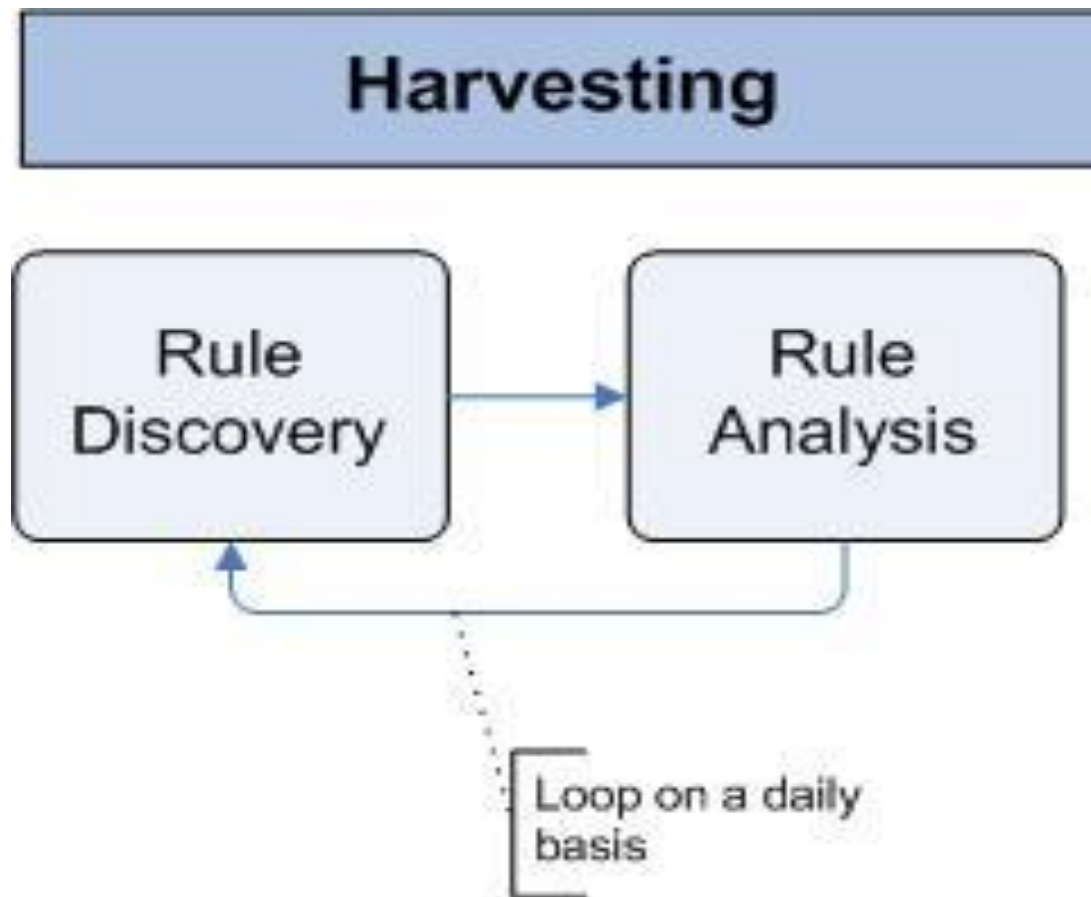
## What a Interoperable Tag Might Look Like:

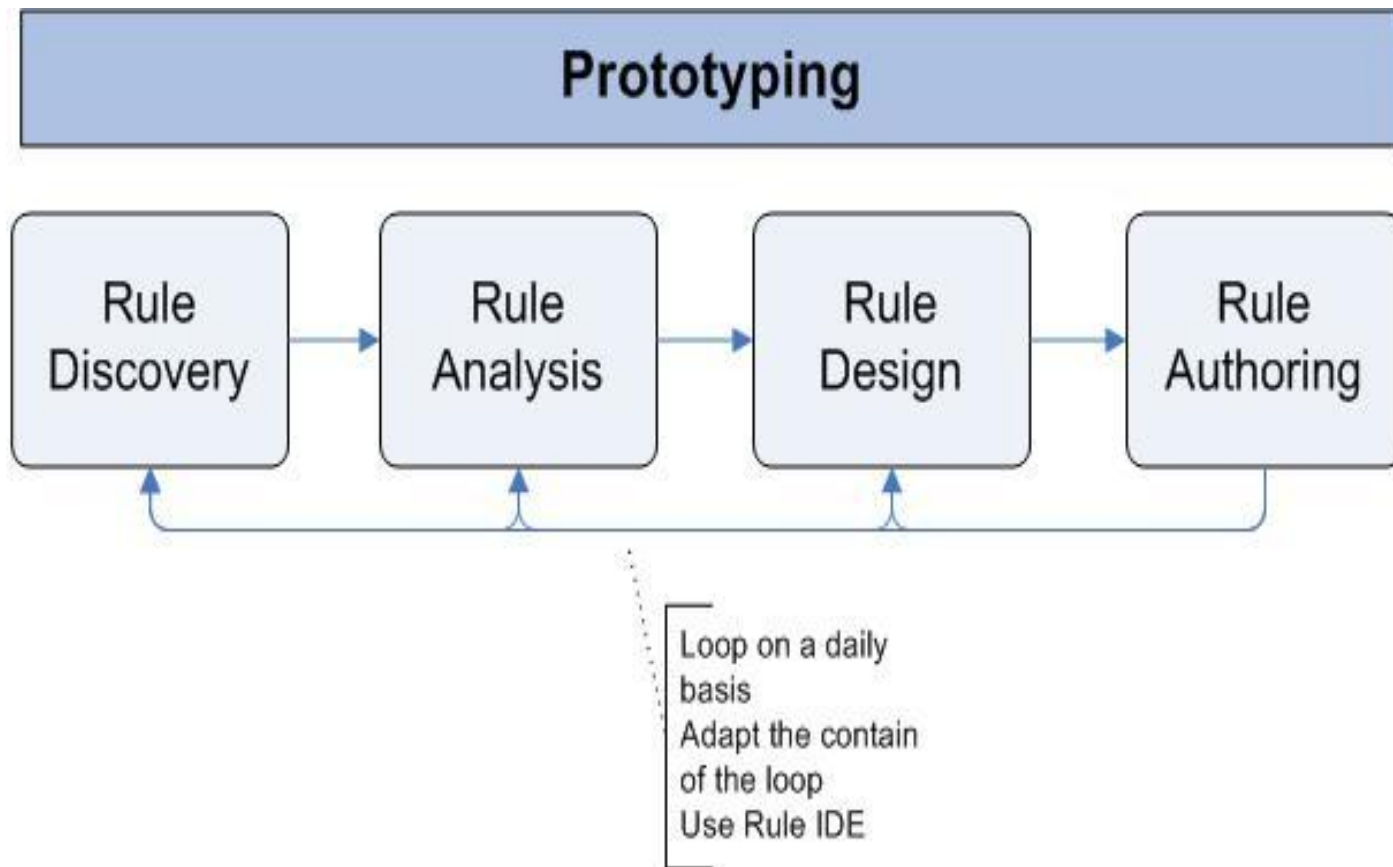
### **For Encounter....**

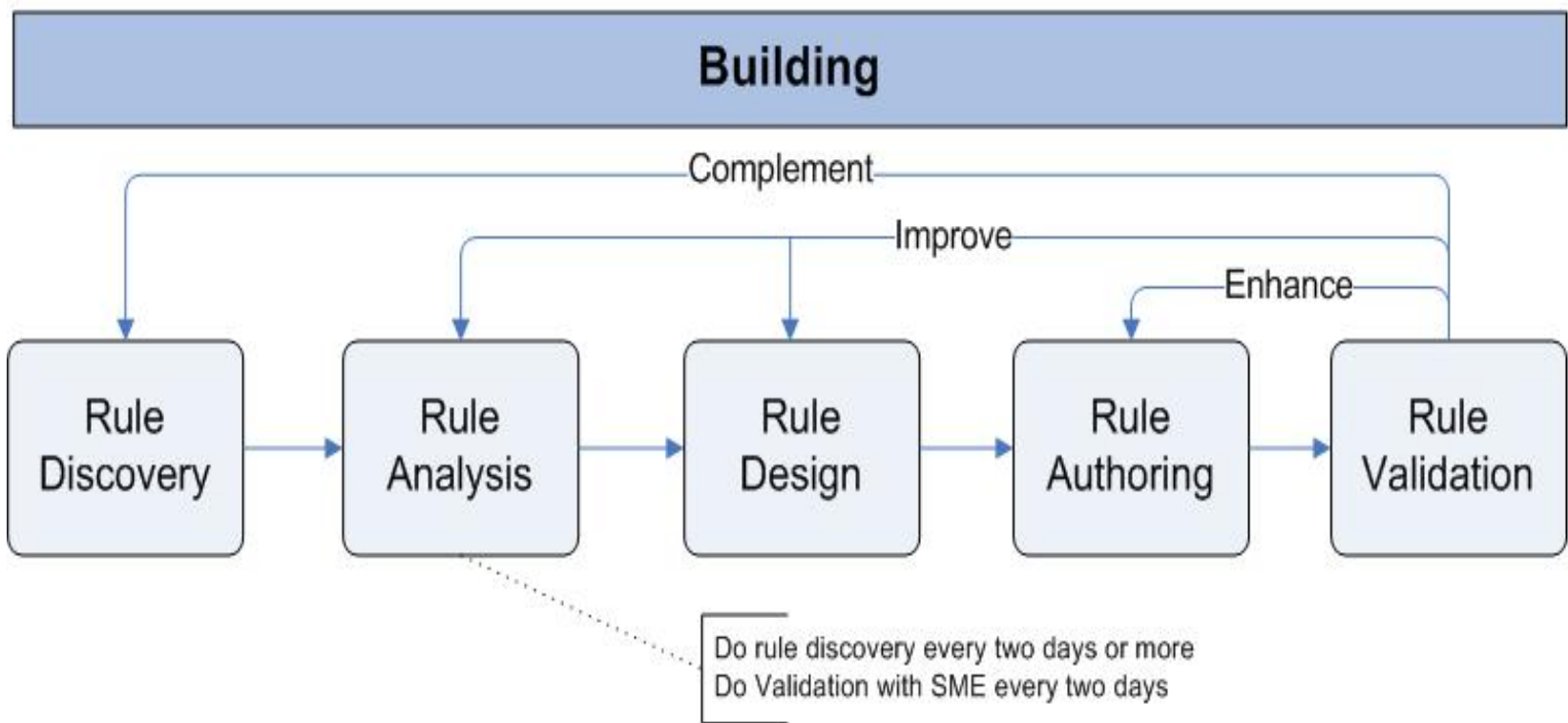
```
<confidentialitytag>  
  <patientId>545482</patientId>  
  <encounterId>10544662</encounterId>  
  <objecttype>encounter</objecttype>  
  <objectid>10544662</objectid>  
  <code>D - Clinician</code>  
  <terminology>  
    <code>1234567890</code>  
    <codeSystem>2.16.840.1.113883.6.101</codeSystem>  
    <codeSystemName>Healthcare Object Taxonomy</codeSystemName>  
    <displayName>Encounter</displayName>  
  </terminology>  
  <datemodified>2011-01-11T04:30:00-04:00</datemodified>  
  <modifiedby>ddecouteau</modifiedby>  
</confidentialitytag>
```

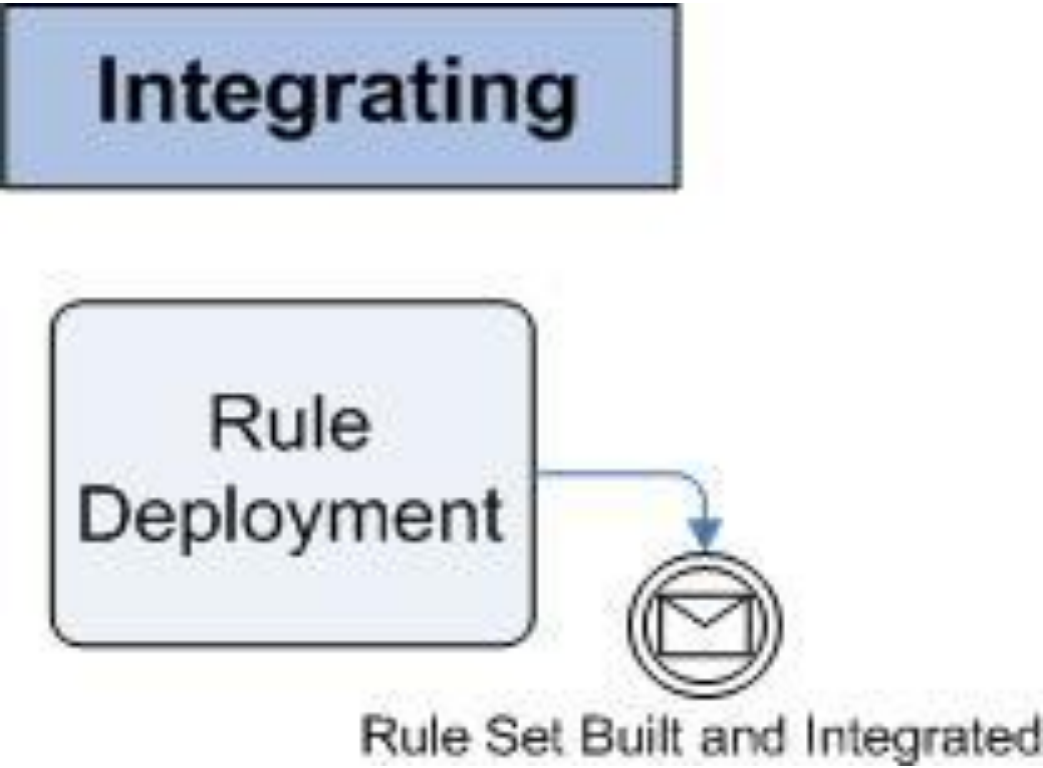


## Phase 1

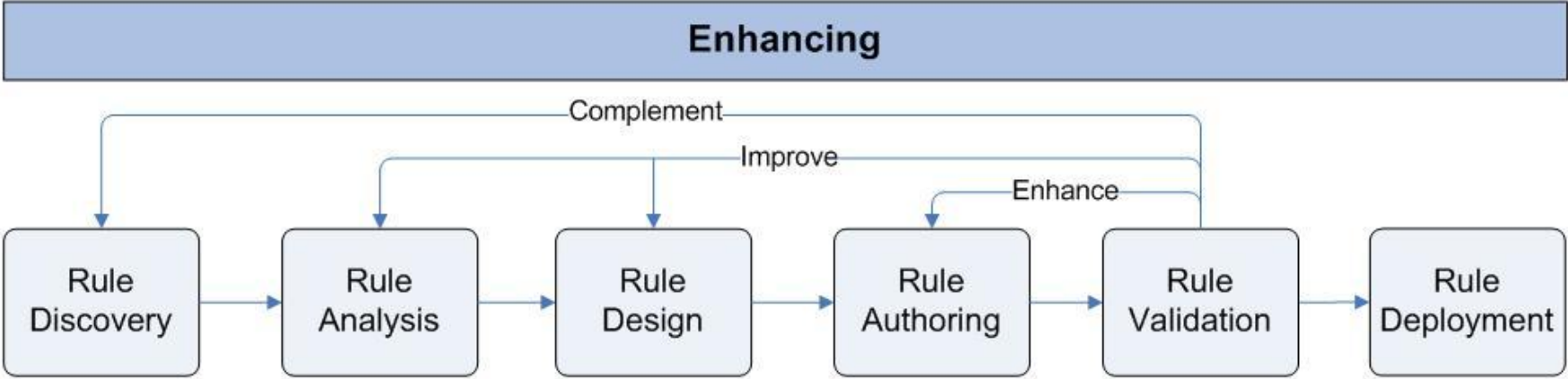


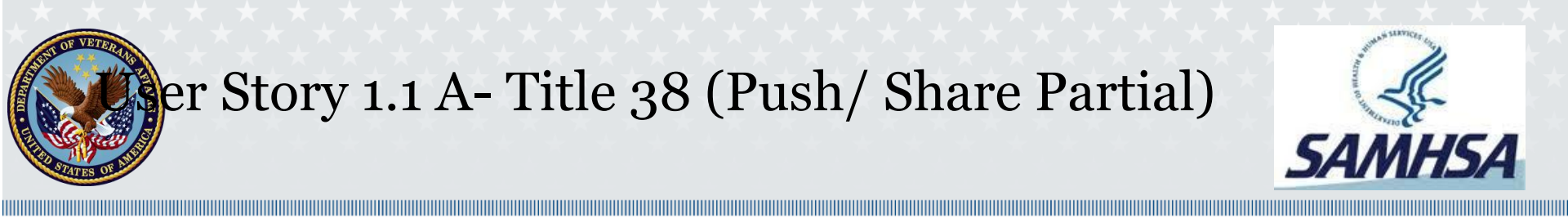






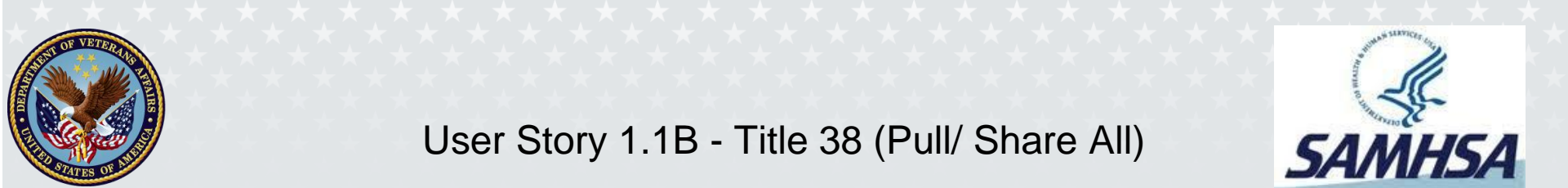






## Case Story 1.1 A- Title 38 (Push/ Share Partial)

- Patient X is admitted to a VAMC for inpatient care for the purpose of treating a 38 CFR Part 1 condition. As Patient X's clinical needs develop, the Patient now requires specialty care.
- The Patient is referred to a Specialist outside of the VA for further care.
- Upon discharge, the VA staff request a 38 CFR Part 1 compliant consent form authorizing the disclosure of 38 CFR part 1 protected ToC clinical data to the Patient's outside Specialist.
- The Patient consents to sharing some (subset) of the protected 38 CFR part 1 data (e.g., medications associated with a covered diagnosis) but does not want to share all of their 38 CFR part 1 covered data. The VA staff electronically captures the Patient consent data.
- The VA electronic system appropriately annotates the Patient data.
- The VA electronically sends (pushes) data for which the Patient has consented to the Specialist (excluding the set of data for which the Patient did not consent to share) with an accompanying compliant 38 CFR Part 1 prohibition on re-disclosure notification.
- The Specialist electronic system receives the Patient's subset data and prohibition on re-disclosure notification.



## User Story 1.1B - Title 38 (Pull/ Share All)

- Patient X is a veteran.
- Before being discharged the VA staff asks the Patient if they would like to share his/her protected 38 CFR Part 1 treatment data.
- The Patient indicates that they would like to share all treatment data with their Specialist.
- The Patient completes a 38 CFR Part 1 compliant consent form authorizing the VA to disclose protected data to the Patient's external Specialist.
- The VA staff electronically captures the Patient consent data.
- The VA electronic system appropriately annotates the Patient data.
- Shortly after being discharged from the VA, Patient X is seen by his/her external Specialist. Patient X informs the Specialist that they were seen at the VA.
- The Patient's Specialist sends an electronic Information request to the VA for the Patient's clinical summary to provide better quality care.
- Because the Patient has signed a 38 CFR Part 1 compliant consent, the VA responds to the information request and electronically sends Patient X's ToC clinical summary, which includes his/her confidential data and an accompanying compliant 38 CFR Part 1 prohibition on re-disclosure notification.
- The Specialist electronic system receives the Patient's ToC clinical summary and Prohibition on re-disclosure notification.

- A Patient in an unconscious state is brought to the local hospital emergency room.
- He/ she is minimally responsive and in a critical state. Identification found on the Patient is used to confirm his/her identity.
- The Emergency Department Physician electronic System electronically sends a breaking the glass request for the Patient's records.
- The responding Organization verifies the request meets emergency guidelines and their electronic system sends the confidential records to the Physician's electronic system, fully recording the conditions of the request and the data provided.
- The ED Physician's electronic system receives the Patients confidential records.

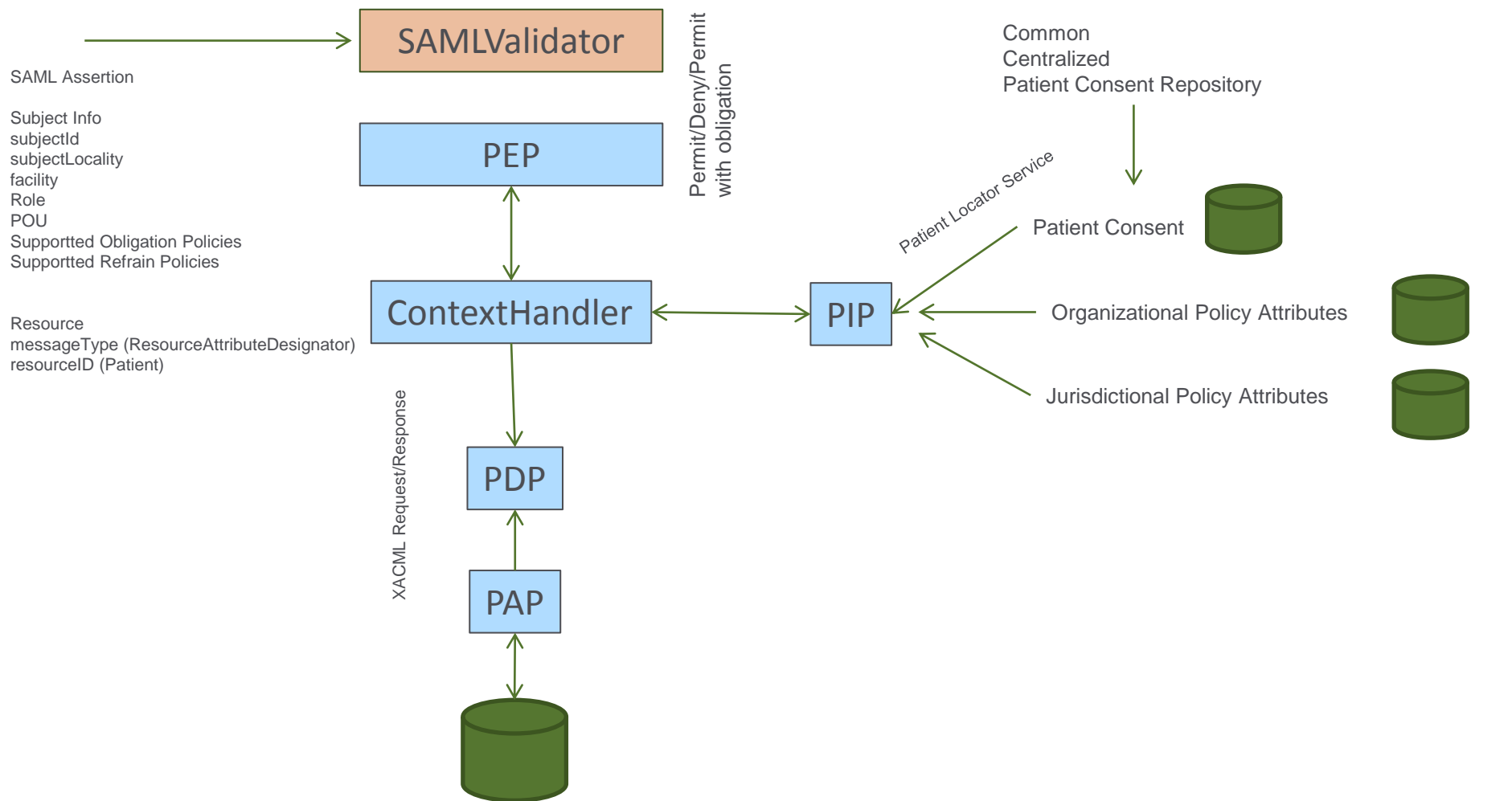
Each disclosure under §§1.460 through 1.499 of this part made with the patient's written consent **must be accompanied by a written statement similar to the following:**

- This information has been disclosed to you from records protected by Federal confidentiality rules (38 CFR Part 1).
- The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 38 CFR Part 1.
- A general authorization for the release of medical or other information is NOT sufficient for this purpose.
- The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient or patient with sickle cell anemia or HIV infection.





## Can The Servicing Organization Provide the Record to Requestor





Can The Doctor Request the Patient Data Locally or Cross - Enterprise

